BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 41-211

13 JANUARY 2011

Health Services

MANAGEMENT OF MEDICAL INFORMATION SERVICES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFMSA/SG6

Supersedes: AFI 41-211, 30 June 1994

Certified by: AF/SG
(Maj Gen Thomas W. Travis)
Pages: 41

This instruction implements Air Force Policy Directive (AFPD) 41-2, Medical Support. It provides requirements and outlines activities, policies, and procedures for Medical Information Services (MIS) Management and identifies integrated planning activities to support the design, development, implementation, and maintenance of automated systems within the Air Force Medical Service (AFMS). It applies to all Air Force (AF) military, civilians, volunteers, students, and contractor personnel under contract by the Department of Defense (DOD) that manage, operate, or utilize services from the medical treatment facility (MTF), Air Force, or other DOD information systems. Unless otherwise specified, the term major command (MAJCOM) includes field operating agencies (FOA) and direct reporting units (DRU). This AFI does not apply to the Air Force Reserve Command or Civil Air Patrol and may be adopted by the Air National Guard. Use of extracts from this instruction is encouraged. Additional instructions and manuals are listed on the Air Force Publishing web site at **http://www.e-publishing.af.mil**. Direct AFI questions, comments, or waiver requests through appropriate MAJCOM/FOA channels to Headquarters Air Force Surgeon General (AFMSA/SG6), 5201 Leesburg Pike, Skyline 3, Suite 1501, Falls Church, VA, 22041 (Note: After September 2011 AFMSA/SG6 will move to: 7700 Arlington Blvd, Falls Church, VA, 22042). Refer recommended changes and questions about this publication to AFMSA/SG6, through appropriate channels, using AF Form 847, Recommendation for Change of Publication. Send any supplements to this publication to AFMSA/SG6, for review, coordination, and approval prior to publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims**/. Public Law 104-13, Paperwork Reduction Act of 1995, and AFI 33-360, Publications and Forms Management, affect this publication. See Attachment 1 for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this instruction does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

Due to significant advancements and ever increasing complexity of Information Management (IM), Information Technology (IT), Information Assurance (IA) and Information Services (IS) within the AFMS, this document was substantially revised and must be completely reviewed. Some major changes include: reorganization of roles and responsibilities, planning, management of support services, information assurance and security, certification and accreditation, information access, data protection, asset management, Health Insurance Portability and Accountability Act (HIPAA) considerations, helpdesk functions, resourcing, IT purchasing, partnerships, responses to information events, and staff competency certification.

Chapter 1

GENERAL INFORMATION

1.1. Overview. Command, Control, Communication, and Computers is vital to all Air Force activities. Healthcare managers throughout the AFMS must have the ability to collect, store, maintain, and retrieve timely and accurate information for planning, organizing, directing, operating, coordinating, and controlling resources in support of patient care, organizational needs and commanders.

1.1.1. This instruction provides guidance, unifying principles, and a minimum set of standardized practices for the planning and execution of IM, IT and IA support programs within the Air Force Medical Service (AFMS). When referencing these support programs within the AFMS, they are collectively referred to as Medical Information Services (MIS). Each requirement, process, and suggested practice outlined in this AFI provides a common vision and understanding for managing MIS requirements and practices at Military Treatment Facilities and ensures standardized MIS support to all AFMS customers.

1.1.2. In cases where an MTF is designated a Limited Scope MTF (LSMTF), the LSMTF will make reasonable efforts to adhere to the requirements of this AFI and identify where resource limitations prevent compliance with any requirement. These limitations must be provided to inspectors in writing at the beginning of inspection activities.

1.2. Roles and Responsibilities.

1.2.1. The Assistant Secretary of the Air Force for Manpower and Reserve Affairs (SAF/MR). SAF/MR serves as an agent of the Secretary and provides guidance, direction, and oversight for all matters pertaining to the formulation, review, and execution of plans, policies, programs, and budgets addressing Health Services. Consistent with SAF/MR Mission Directive 1-24.

1.2.2. Air Force Medical Support Agency (AFMSA). AFMSA provides the first level of corporate oversight for planning, programming, budgeting and execution activities related to medical modernization. The directorate works with Functional Area Working Groups, Integrated Process Teams, Direct Reporting Units, and Field Operating Agencies / MAJCOMs that require corporate review.

1.2.2.1. Provides direction, policy, and resources to leverage science, technology, and industry transformation and modernization in medical capabilities.

1.2.2.2. Addresses medical system and software standardization and integration in support of Air Force medical and line commander operations.

1.2.2.3. Advises the AF Surgeon General, Military Health System (MHS) and other federal agency leaders on MIS matters.

1.2.3. AFMS Office of Chief Information Officer (SG6). The AFMS Chief Information Officer (CIO) is responsible for all MIS policies, plans and related items. The AFMS CIO also advises the AF/SG and executive staff on all MIS matters and develops a professional MIS workforce.

1.2.3.1. Oversees and utilizes resources in the AF/SG6 directorate to accomplish MIS strategic planning, system integration, and acquisitions. Directs AFMS Portfolio Management and Enterprise Architecture activities, coordinates strategy as needed with the AF CIO, MHS CIO, Office of the Assistant Secretary of Defense (Health Affairs), Army and Navy medical commands, and other federal health leaders/partners. For further information refer to paragraph 1.2.4. and online resources located at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=SGROCC** and on the AFMS CIO Knowledge Junction at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=AFMSChiefInfoOfficer**.

1.2.3.2. Establishes working relationships with, and advocates AFMS needs to SAF/CIO A6, Office of Warfighting Integration and Information Dominance, Air Force Space Command (AFSPC) Air Force Network Operations Center, Air Force Network Integration Center (AFNIC), Air Force Enterprise Configuration Management Office, MAJCOM/A6, and local Communication Squadrons (CS).

1.2.3.3. Ensures a blending of medical mission requirements and network security policies, procedures, and efficiencies.

1.2.3.4. Manages the DOD Information Assurance Certification and Accreditation Process (DIACAP) outlined in DODI 8260.04, Military Health System (MHS) Support to DoD Strategic Analysis, for all MHS and AFMS medical applications/systems installed at AF MTFs IAW applicable directives. See Attachment 1.

1.2.3.5. Develops automated health data analysis tools and measures for executive decision support. Performs medical analytics in accordance with DOD Instruction 8260.04, Military Health System Support to DOD Strategic Analysis.

1.2.3.6. Oversees, formulates, and consults policy for the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security provisions IAW DOD 8580.02-R, DOD Health Information Security Regulation, DOD and AF directives.

1.2.4. Air Force Medical Support Agency SG6 Divisions. AFMSA/SG6 Office of the AFMS CIO consists of multiple divisions. These divisions perform planning, policy, and support for MIS that is aligned with the AFMS Strategic Plan, AFMS Enterprise Architecture, AFMS Portfolio Management and TRICARE Management Activity (TMA) directives. For further information, see online resources located at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=SGROCC** and on the AFMS CIO Knowledge Junction at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=AFMSChiefInfoOfficer**

1.2.4.1. SG6 divisions provide services, assets, and coordination activities that meet or exceed customer information needs. The primary objective is to support the health and welfare of the war-fighter and beneficiaries by implementing military health information technology (HIT), developing and revising policies, integrating clinical and business technology advancements and governance, validating new requirements and ensuring compatibility for the AFMS enterprise.

1.2.5. Surgeon General's Requirements for Operational Capabilities Council (SGROCC) and Capabilities Review and Risk Assessment Processes.

1.2.5.1. Provides review, integration, and validation of all Air Force medically relevant expeditionary, business and clinical capability requirements for the AFMS corporate structure.

1.2.5.2. Provides an effective, systematic way to review AFMS capability gaps. Those requiring a materiel solution are brought from concept to fully developed, deployed systems in support of the health and welfare of the war-fighter and eligible healthcare beneficiaries. For details on submitting new requirements/capabilities, go to the SGROCC website located at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=SGROCC**.

1.2.5.3. Decreases the amount of redundant products/processes and ensures thorough analysis of alternative to ensure issues/concerns are addressed early in development.

1.2.5.4. Ensures Initial Capabilities Documents (ICD) and Capabilities Development Documents (CDD) are developed. All new initiatives and capabilities are sent to the IM/IT or Modernization Panel for funding consideration.

1.2.6. Air Force Medical Operations Agency (AFMOA) IS Division/MAJCOM CIO.

1.2.6.1. Leads, plans, assists, and educates MTFs and medical DRUs to deploy and sustain efficient MIS operations. Serves as the first line of resourcing and support for daily medical unit IS execution activities.

1.2.6.2. Advises MAJCOM SGs, AFMSA/CC, AFMOA/CC, and AFMS CIO on all MTF/DRU requirements and issues relating to planning, system integration, interagency cooperation, data, voice and video communication infrastructure, equipment procurement/refresh and customer support.

1.2.6.3. Gathers and relays inputs on policy and guidance from MTFs and medical DRUs to AFMSA.

1.2.6.4. Plans budget requirements, standardizes processes/configurations and coordinates system implementation across the AFMS in conjunction with AFMSA/SG6 and AFMS Strategic Plan, AFMS Enterprise Architecture, AFMS Portfolio Management and TMA directives.

1.2.6.5. Supports data quality, modeling and analysis activities, sharing these responsibilities with other applicable AFMOA divisions and AFMSA/SG6 divisions.

1.2.6.6. Provides contract support for medical and technical services and serves as a consultant to the Requirements Assessment Team (RAT) for developing, testing and evaluating initiatives.

1.2.6.7. Establishes working relationships with respective MAJCOM and AFMOA service provider counterparts to ensure integration of medical mission requirements and network security policies, procedures and efficiencies. Encourage standardization of IT service levels which are typically handled differently by each MAJCOM and/or base.

1.2.6.8. Manages the Quarterly Enterprise Buying (QEB) program for the AFMS. Utilizes historical data to ensure MTFs are adequately refreshed with IT hardware assets within established policies and approved exceptions.

1.2.6.9. Serves as the communication conduit between program managers (PM) and MTFs. Proposed or scheduled actions that impact MTFs should simultaneously flow from the PM to AFMOA/MAJCOM and MTFs. This provides an opportunity for AFMOA to balance and coordinate any actions/requests against other ongoing activities.

1.2.6.10. Serves as a central collection point for data call inquiries sent to the MTF on behalf of MAJCOMs or at the request of higher headquarters.

1.2.6.11. Performs site visits when requested by MTFs or higher headquarters. Site visits are requested through the MTF commander or MAJCOM staff and submitted to AFMOA. Reasons for site visits may include problem resolution, pending inspections, advice and consultation and high staff turnover.

1.2.7. Medical Information Services (MIS) Flight Commander (SGSI), or Equivalent. The MIS Flight Commander is responsible for all MIS activities in the MTF and serves as the Chief Information Officer for the organization. The CIO is a visible member in all functional areas and actively engaged in all sections of the MTF. The following duties and responsibilities can be appropriately shared with the MIS Flight Commander’s Deputy or Flight Chief/NCOIC.

1.2.7.1. Periodically briefs and advises the MTF Commander and executive staff on the status of information systems, services, initiatives, and needs.

1.2.7.2. Manages the installation and lifecycle of all MTF IS and applications.

1.2.7.3. Manages life cycle and inventory for all organizational IT resources.

1.2.7.4. Coordinates with AFMOA/MAJCOM on MIS policy, budgeting, standardization, and system implementation.

1.2.7.5. Gathers and elevates MTF requirements for purchases of end-user devices (desktops, laptops, tablets), servers, printers, personal electronic devices (PEDs), land mobile radios (LMRs), audiovisual equipment, telecommunications and cable plant for MIS components.

1.2.7.6. Maintains a helpdesk function to serve as on-site support for all MIS issues. Ensures helpdesk utilizes an automated trouble ticketing system to document and track all MIS trouble tickets. Leverages centralized helpdesk functions, tools, or procedural directives when and where available.

1.2.7.7. Supports data quality, data mining and reporting activities but may share these responsibilities with other sections within the MTF.

1.2.7.8. Serves as the IM project champion or co-champion for Joint Commission (JC), Accreditation Association for Ambulatory Health Care (AAAHC), Health Services Inspection (HSI), and other facility compliance inspections. Conducts annual MIS needs assessment and advises the Executive Committee concerning findings, action plans and process improvements as they relate to mission accomplishment and inspection standards.

1.2.7.9. Manages and enforces software and hardware DIACAP requirements and compliance for all MTF applications installed or projected to be installed IAW AFI 33-114, Software Management, and AFI 33-200, Information Assurance (IA) Management.

1.2.7.10. Ensures non-authorized software are removed from all IT end-user devices and servers in accordance with IA policies and procedures.

1.2.7.11. Establishes programs, procedures, and end-user agreements to ensure individual accountability for safeguarding and securing desktop equipment, mobile devices and PEDs.

1.2.7.12. Supports telephone, cell phone, pager, and LMR management and may share these responsibilities with other sections within the MTF.

1.2.7.13. Obtains and maintains a Secure Internet Protocol Router (SIPR) account to receive classified network notifications.

1.2.7.14. Maintains, tracks, and reports required and optional MIS staff training and compliance. (e.g. Systems V4A0X1, and 8570 certifications)

1.2.7.15. Understands and complies with applicable MIS directives. Directives can include, but are not limited to, AFIs, AFPDs, AFMANs, AFSSIs, DOD instructions, Notices to Airmen (NOTAMs), Maintenance Tasking Orders (MTOs), Time Compliance Network Order (TCNO), Security Technical Implementation Guides (STIG), and Warning Orders. See partial list of references in Attachment 1. Oversees, formulates, or consults on policy implementation based on these provisions.

1.2.7.16. Establishes working relationship with local Communications Squadron counterparts and appropriate functional areas such as Asset Management, Comm Focal Point (Help Desk/Network Control Center), Contracting, Telephone Ops, Frequency Management etc.

1.2.7.17. Establishes working relationships with respective Medical Logistics, BioMedical Equipment Repair, MAJCOM/AFMOA counterparts to ensure integration of medical mission requirements, contracting, network security policies, procedures and efficiencies.

1.2.7.18. Fosters and improves standardization and integration of IT equipment and services across the spectrum of hospital and clinic operations in accordance with the organizational goals, the AFMS Strategic Plan, and Enterprise Architecture, Portfolio Management and TMA directives.

1.2.8. End User.

1.2.8.1. Must adhere to password and network security policies and protect physical access to network resources at all times.

1.2.8.2. Comply with annual information protection, information assurance, and HIPAA training requirements and guidance.

1.2.8.3. Understand and protect sensitive information. Prevent and report unauthorized release or compromise of data or information, whether on or off the electronic network.

1.2.8.4. Safeguard and adhere to all stipulations in end-user agreements for fixed and/or mobile hardware devices assigned.

1.2.8.5. Read, understand, and comply with all responsibility and accountability provisions in the standardized DOD End-User Agreement. This agreement will be physically signed by end-user and acknowledged within the network pop-up banner upon initial and subsequent logons.

Chapter 2

MEDICAL INFORMATION SERVICES

2.1. Overview. Medical Information Services (MIS) must support the Medical Communications and Information (C&I) spectrum and continually adapt to technology and policy changes. The primary C&I support components provided by the MTF MIS Flight are: system installation and/or installation assistance; technology operations and maintenance; system utilization guidance; lifecycle management (upgrade, replacement, budgeting), problem resolution, and physical and logical security of MTF hardware, software, local area network (LAN) and information resources. Providing this support requires a collaborative and coordinated effort between various individuals, entities, and agencies, including but not limited to; Network Administrators, Communications Squadrons, Integrated Network Operations and Security Centers (INOSCs), Client Support Technicians (CSTs); Functional System Administrators (FSAs), Medical Logistics, Facilities Management, Medical Equipment Management Office, Medical Resource Management, Air Force Medical Operations Agency, Air Force Medical Support Agency, Military Health System Helpdesk, Medical Cyber Infrastructure Services (MCiS, previously TIMPO), and system vendors. The MIS flight is responsible for facilitating, collaborating and coordinating with these entities to provide reliable information services.

2.2. Core Services. Public webpage hosting, e-mail, print and file services, domain controllers, domain naming servers, dynamic host control, network/e-mail user accounts, and network/boundary device (routers, switches, firewalls, intrusion detection) management are “core services” and components of the AF Global Information Grid (AFGIG). With few exceptions, these services are normally, and should be, provided by Line Air Force (LAF) C&I counterparts (Communications Squadrons [CS] and/or INOSCs). Core services are defined in AFI 33-115v1, Network Operations, Chapter 6 and are provided using network administration, remote management, consolidated hosting, and information protection tools. Core services do not normally include unique medical application administration and maintenance of systems fielded by MHS or the AFMS. Specific or unique local medical server configurations and local core service network support needs should be discussed with local CS and specified within a Service Level Agreement (SLA). (See Chapter 10, Service Level Agreements)

2.3. Hardware. Hardware includes all physical devices or assets used in electronic information processing. Strict control of IT assets, also referred to as Automated Data Processing Equipment (ADPE) is integral to controlling overall IT costs. The MIS flight shall ensure effective processes and procedures are in place and followed for acquiring, receiving, labeling, inventorying, tracking and disposing of ADPE. ADPE management and tracking should be closely coordinated with the local CS, Medical Logistics, and the Medical Equipment Management Office (MEMO) where applicable. Desktops, laptops, tablet PCs, monitors, printers, scanners, servers, personal digital assistants (PDAs), telephony equipment, back-up and storage equipment (Storage Area Network and Network Attached Storage), uninterruptible power supplies, wireless infrastructure devices (antennas, controllers), network appliances (switches, routers, hubs), and other medical automated information systems (AIS) hardware represent a large AFMS investment and are examples of the types of assets that should be closely tracked and managed. (See Chapter 5, IT Asset Management.)

2.4. Software. Software includes all sets of information processing instructions, operating systems and applications. All software, whether developed within the government (government off-the-shelf [GOTS]) for Air Force or DOD purposes or procured commercially off-the-shelf (COTS) must be managed and used effectively to prevent violations of copyright laws, end-user, and enterprise license agreements. This includes, but is not limited to, information assurance (patch, upgrade, and configuration management), and license management (tracking, assignment, reuse, expiration, renewal). It is incumbent on the MIS Flight to understand what software is licensed to the enterprise and track locally procured software licenses. Further guidance on software management can be obtained in AFI 33-114.

2.5. Network. Data and telecommunications technologies and networks (e.g. Internet, intranet, extranet, LAN, WAN) are essential to successful electronic business operations of the MTF. Network cabling, electronics, wireless antennas, controllers, and telephone call distribution systems provide the fundamental infrastructure to support all MIS C&I and should be protected as strategic resources. MTFs should expect their network cable plant and electronics to be modernized every five to seven years by the AFMSA Medical Systems Infrastructure Modernization (MSIM) team. MSIM schedules are updated and coordinated through the MAJCOM/FOA. Although overall network resource management is conducted outside the healthcare organization by communications agencies there are still important roles and responsibilities at the MTF. AFI 33-115, Volume 1, Network Operations, Chapter 13, provides detailed guidance for effective network resource management. Due to the importance of these resources, the MTF should strive to obtain and maintain an experienced network administrator to provide responsive support and subject matter expertise and advice to MTF leadership.

2.6. Consolidation and Management Initiatives. Advances in security configurations, monitoring, remote administration, and IT Infrastructure Library (ITIL) standards have moved the Air Force toward IM/IT/IS consolidation. Consolidation projects and other centralized IT management and administration initiatives should be carefully planned in conjunction with local CS, INOSC, and AFMOA personnel. In each case a detailed plan and phased approach should identify and mitigate operational risks. The project end-state should sustain and ultimately improve reliability, availability, or performance of MIS to the MTF during and after migration or implementation. Significant initiatives should trigger adjustments to an existing SLA or a new SLA with the CS. CS and MTF expectations about final outcomes should be understood and clarified in writing prior to executing new migration or consolidation initiatives. (See Chapter 10, Service Level Agreements)

2.6.1. HIPAA Considerations: When planning for server or storage migration, the MIS Flight Chief must assess what type of data is being stored on the file servers. Server used to manage or store Protected Health Information (PHI) or Personally Identifiable Health Information (PII) supporting medical programs will be logically (electronic storage schema) consolidated and protected. MIS leadership should consult MAJCOM/AFMOA and Medical Legal Consultants prior to physical server consolidation efforts outside of the MTF to ensure HIPAA compliance. (See Chapter 7, HIPAA Security).

2.7. Helpdesk Operations. Every MTF MIS Flight should provide on-site helpdesk services during normal business hours. Larger MTFs with 24-hour inpatient and/or emergency services should have 24-hour IT help or after duty hours IT service on-call coverage. The helpdesk answers and resolves issues at the lowest level possible. Each work order (trouble tickets) shall be documented to accurately capture workload. If mission and scope change, accurate workload data are essential to justify additional staffing, technology acquisition, and fiscal resources. Local MTF helpdesk tickets elevated to the local CS should be tracked and updated in the local system. Where possible a common or centralized ticketing system should be used.

2.7.1. Helpdesk Contact. Each MIS Flight will have a dedicated published helpdesk phone number and organizational e-mail box for customers to submit helpdesk requests. When and where available MIS flights should leverage centralized/enterprise helpdesk services and migrate local ticketing systems to common or centralized enterprise ticketing systems. During non-duty hours or when in use, the helpdesk line should roll over to a voice mail message that describes emergency/alternate contact procedures and/or central helpdesk contact information.

2.7.2. Work Orders. Customer helpdesk support requests shall be logged and receive a unique work order number. The customer should be informed of resolution progress thereafter, until the ticket is closed, with complete documentation in the resolution section of the work order. In the case of projects, status updates should also be made regularly to the customer. Work order status must be consistently and reliably updated by the MIS or centralized helpdesk. Work orders are not closed without final consultation with the customer to ensure problem was resolved satisfactorily.

2.7.3. Support Tiers. Tiers 0 – 3 are used in the helpdesk environment. Tier 0 problem can be resolved through self-service methods. Tier 1 problems are resolved by helpdesk personnel via telephone or remote management assistance and consist of a Problem Type and a Category. The Tier 1 level may be at a central location or at the local MTF. Tier 2 problems usually involve hands on assistance by the MTF helpdesk staff or local CST/FSA with the user due to the complexity of the issue. Tier 3 problems are escalated to resources outside the MTF, such as the Network Control Center (NCC), the MAJCOM/AFMOA, Standard Systems Group (SSG) at Gunter Annex, MHS Helpdesk, or the system vendor.

2.7.3.1. Work Order Priorities. In a medical environment typically there are three main priorities assigned to IT work orders/trouble tickets. General definitions and associated response times are (1) immediate (e.g. clinical/patient care work stoppage, 15 minutes), (2) elevated (e.g. degradation of work flow, within1 hour), and (3) normal (e.g. all other routine, 2 hours). Any work order can be any priority. “Response time” should be calculated from initial customer contact. The definitions of the priorities with the response times should be advertised to the MTF staff and MIS extenders. The MTF CIO must educate customers on work order priority and expected service response times.

2.7.3.2. Work orders related to core services are handled through the Communications Focal Point (CFP) or CS consolidated helpdesk and should be monitored to completion by the MIS Flight helpdesk.

2.8. Telephone Services. The MIS Flight in conjunction with facility management section provides management oversight for the MTF telephony requirements. The local CS provides functional (e.g., touch labor) support for the MTF portion of the base telephone system. Depending on the MTF, the MIS Flight may be responsible for coordinating day-to-day work orders, call tree/menu changes, levels of service, and performance metrics with the local CS. The MIS Flight, through the Telephone Control Officer, is responsible for reconciling invoices. In some MTFs the aforementioned responsibilities may be shared with other sections such as Medical Logistics or Facility Management.

2.8.1. In most cases the local CS is responsible for managing and servicing telephone switches and trunk lines, and ensuring appropriate telephone support to the MTF. In certain circumstances, some MTFs may physically house telephone switching equipment and/or automated call distribution systems. In such cases agreements should be in-place between the MTF and the CS to clarify operation, maintenance, and replacement responsibilities.

2.8.2. Telephony Modernization (TELMOD). Telephone support and telephone equipment lifecycle activities should be managed by the local CS with oversight, monitoring and coordination through the MIS Flight. Although the MIS Flight is not normally responsible for setting up or modifying logical call tree design, they usually serve as the interface between the responsible POC and CS for implementing those changes. To ensure clarity of responsibilities for telephone equipment support the MTF and local CS should create a SLA for telephone equipment. An SLA should define responsibilities and clarify ownership/roles for support, maintenance, sustainment, and overall life-cycle management of telephone system hardware and functions. Sample SLAs for TELMOD can be found on AFMOA's website at **https://vc.afms.mil/AFMOA/default.aspx**.

Chapter 3

MANAGEMENT OF MEDICAL INFORMATION SERVICES

3.1. General Information. The MTF MIS Flight Commander or equivalent is responsible for managing MIS operations and planning activities within the organization. He/she must continually assess operations, direct resources, forecast needs, and plan for the future. Although MTF MIS Flights/Elements are organized in various ways throughout the AFMS most have a senior enlisted member or Civil Service (government) equivalent to help with day-to-day operations and management. Each flight should have an experienced network administrator to provide technical expertise and help act as liaison with local communications personnel.

3.2. Management Functions. MIS Flights must carefully manage resources and perform a variety of functions to meet the IM/IT and communication needs of internal and external customers. When appropriately managed, each of the following areas will enhance the MIS Flight's efficiency and effectiveness.

3.2.1. Financial Resources. Staff should maintain awareness of MTF/DRU annual budget requirements and forecasts, quarterly spend rates, projected funding needs, contracts and opportunities for unfunded requirements to meet organizational MIS and system lifecycle management needs. Communicate financial and contracting needs to Resource Management Office (RMO), Logistics, and AFMOA as early as possible.

3.2.2. Human Resources. MIS authorized staff positions should be filled and utilized in the appropriate Functional Area Code to ensure required resources are available for MIS operations. Staffing size and skill mix may vary from one MTF to another depending on the size, host/node relationship to geographically separated MTFs and locally funded contracts. Additional support and optimization of MIS Flight staff can be achieved by managing MIS extender and training programs. Obtaining the right staffing levels and mix of military, civil service and contractor support is a key to operational success. (See Chapter 4, Staffing.)

3.2.2.1. MIS Extenders. Increasing workload and staff shortages may necessitate the MIS Flight's use of qualified MIS Extenders throughout the MTF as IT support assistants. Having CSTs, Information Assurance Officers, and FSAs in key sections within the MTF can help alleviate helpdesk bottlenecks and decrease service response times. MIS Flight commanders should evaluate the need for extenders. If needed, an extender program should have the support of MTF executive team. The MIS Extender program should include assignment letters, extender training, guidance on responsibilities and procedures, a training tracking mechanism, e-mail group for notifications, and regularly scheduled informational meetings. An MIS Flight staff member will monitor and manage the MIS extender program.

3.2.2.2. Skills and Training. Developing a skill requirements matrix allows MIS Flights to identify current skill sets and plan for skill shortfalls. The MIS Flight Commander or equivalent should have a thorough understanding of the Enlisted Evaluation System, civilian personnel management systems, Quality Assurance Personnel program, DOD 8570.01-M, Information Assurance Workforce Improvement Program requirements for military, civilian, and contract personnel. They should seek and enroll staff in local training opportunities such as CST, FSA, IT E-Learning and Microsoft application classes. Officers will attend the Medical Information Services Orientation Course upon initial MIS assignment. Enlisted members who are assigned to a corresponding position on the Unit Manning Document (UMD) are eligible for the V-prefix and can register for the computer-based training plan on the Air Force IT E-Learning/Skillport website at **https://www.my.af.mil/skillportcbtprod4/skillportfe/main.action?selectedTab=1**.

3.2.2.3. Career Development. Career development is important for officers, civilians, and enlisted members in the MIS career field. Both officer and enlisted career field managers have specific requirements to obtain the V-prefix. Officer and Enlisted personnel should reference AFI 36-2101, Classifying Military Personnel (Officer and Enlisted). Officers should reference the Air Force Officer Classification Directory, and enlisted members should reference the 4A0X1 Career Field Education and Training Plan on the Air Force Personnel Center website for the specific criteria necessary to obtain the V prefix. The decision to send members to free, paid, or optional training should be weighed carefully with the needs of the Air Force/MTF, and consider individual desires and motivation, length of remaining service commitments, and applicability of training to duties.

3.2.3. Data and Information. Data and information must be managed effectively to benefit organizational end-users. Effective data resource management ensures electronic data is secure, available, screened for quality, backed-up, and can be recovered in a timely manner. Back-up and recovery plans should be documented. AFPD 33-3, Information Management, provides general guidance with references to other applicable instructions and policies. AFI 41-217, Health Information Assurance for Military Treatment Facilities, provides more specific information for health-related data resource management, security and safeguarding of protected health information.

3.3. Management Tools. Use of the following tools and concepts can enhance MIS management efficiency and effectiveness.

3.3.1. Process Models. Applying simple Air Force process models such as Plan, Do, Study, Act (PDSA) or Observe, Orient, Decide, Act (OODA Loop), and/or more in-depth models such as the System Development Lifecycle (SDLC) process will enhance MIS capabilities and ensure resources are aligned with organizational needs.

3.3.2. Information Capital. The MIS Flight Commander or equivalent has many information resources and tools to manage information systems and must be familiar with information sources, such as the self inspection checklist, HSI checklist(s), Joint Commission and Accreditation Association for Ambulatory Health Care (AAAHC) IM standards, needs assessments, Air Force, trade, and private sector publications, online resources, AFIs, AFPD, and AFMANS.

3.3.3. Needs Assessment. A needs assessment will be accomplished annually. The needs assessment will help identify and prioritize new requirements. The annual needs assessment is an excellent planning tool and helps reinforce the strategic importance of the MIS Plan. The assessment should aggregate quantitative and qualitative data gathered from surveys, helpdesk system reports, committee minutes, and interviews with staff. A needs assessment is not just an IT focused survey; it should gather feedback on information products, processes, and services. There is no specified format however Needs Assessment examples may be found at AFMOA online resources. Analysis of results should lead to formulation of action items that are summarized, prioritized, and presented directly to the Executive Committee or the IMC/F.

3.3.4. Performance Metrics. The MIS Flight Commander or equivalent implements performance metrics to track the quality of service provided to the MTF. Tracked metrics should include, but are not limited to, average daily/weekly/monthly work orders, average work order resolution times, end user satisfaction levels, percentage of first call resolution, key application availability, network availability, total MIS staff/total user ratio, and information protection training compliance.

3.3.5. Customer Service. Competing priorities and resources should be carefully managed so they do not create barriers to good customer service. Good customer service is an effective management tool and an ally to the MIS Flight. A reputation of good service will lead to added credibility when competing for resources and MIS staff time savings from reduced complaints. The entire MIS Flight staff should practice and foster an attitude of excellent customer service. Where and when possible MIS Flights should establish flexible and responsive service models (e.g., roving technicians, customer follow-up, 24-hour or extended hour service, first call resolution) as well as customer satisfaction metrics.

3.3.6. Policy and Guidance. MIS Flights should consider establishing local MIS policies, guidance, or instructions. Examples may include IT equipment and system acquisition, equipment inventory and tracking, policing of non-mission essential storage, e-mail etiquette and internet utilization. Guidance on some of these functions may be provided by the local CS or higher headquarters. When managing these functions within the MTF local procedures should only compliment base, MAJCOM/AFMOA, AF, DOD guidance and instructions. The overall focus should be to ensure Air Force Medical Service IT equipment, storage, network resources, and bandwidth are utilized and available for mission essential tasks. Strict policing, enforcement, and accountability for local procedures will help reduce their use for non-mission essential activities. Documenting policies and/or guidance in a Medical Group Instruction, Operating Instruction, local Medical Group policy/guidance letter(s) or another appropriate format is recommended.

3.3.7. Automation Tools. Leveraging approved automated hardware and software tools or configurations can greatly enhance MIS presence and breadth of services. Examples are asset inventory systems, work order databases, e-mail work-flow boxes, online survey services, call forwarding, linked spreadsheets/metric charts, push reports, network traffic/bandwidth monitoring, scanning, electronic auditing, project management applications, remote environmental monitoring, notification, content management tools, etc. MIS Flights should consider sensible use of automation tools especially where time and money savings can be attained.

3.4. Planning and Oversight. Managing planning and oversight functions include:

3.4.1. Medical Information Services Plan. The MIS Flight Commander or equivalent is the MIS subject matter expert (SME) within the MTF. Although NOT mandatory it is advisable that the MIS Flight Commander create and update an MIS plan. There is no specified format or length for an MIS plan however it may be beneficial to maintain the plan in a slide or briefing format. The plan should contain strategic MIS goals and objectives that support organizational needs and align with organizational and AFMS missions, visions, strategies and priorities contained in the AFMS Futures Support Plan found at

https://kx.afms.mil/sgcag. The plan should identify manpower and fiscal resources required to implement current requirements and future IM/IT initiatives projected for one to five years. The MIS Flight Commander or equivalent can utilize an MIS plan to update the Executive Committee or Information Management Function/Committee (IMF/C) on progress. Considerations for MIS plan content would include workload metrics, lists of sustained programs, plans/schedules for new systems and upgrades, and recommendations on maintaining, resourcing, and enhancing existing MIS operations as drawn from an annual needs assessment.

3.4.2. Information Management Function/Committee. The IMF/C is a function that serves as an advisory body on Joint Commission and AAAHC inspection standards related to information management and technology. The MTF Administrator normally chairs the IMF/C but can delegate this role to the MIS Flight Commander or equivalent. The chair or delegate is responsible for setting the agenda, recording attendance, inviting speakers and preparing meeting minutes. Minutes are coordinated IAW MDG committee guidelines. The IMF/C reviews MIS processes and resources to ensure information is used and communicated effectively throughout the organization. IMF/C members, clinical, surgical, diagnostic, and ancillary functional areas jointly establish and update an Information Management Plan (IMP). (See IMP Section below)

3.4.2.1. The IMF/C is a cross-functional team comprised of executive, administrative and clinical members. The following areas/sections are an integral part of the IMF/C however ongoing membership is at the discretion of the MTF Administrator: Medical Group and Squadron Commanders, Medical Information Services, Resource Management, TRICARE and/or Patient Administration, Coders and/or Auditors, Medical Expense Performance Reporting System Manager, Defense Medical Human Resources System-Internet Program Manager, Data Quality Manager, Credentialing, Patient Safety, Group Practice Manager, Health Care Integrator, HIPAA Privacy and Security Officers, clinical practitioners, and Medical Information Security Readiness Team (MISRT) Representative.

3.4.2.2. At a minimum the IMF/C should meet semi-annually to identify, discuss, and decide on information management programs, projects, initiatives, shortfalls, concerns, and needs. IMF/C minutes should document resolution and process improvement actions taken for JC review.

3.4.3. Information Management Plan (IMP). The IMP should outline key clinical and business process information flows within the clinic or hospital. There is no specified template but IMP tools may include bullet documents, flowcharts, spreadsheets, or presentations. The plan should describe key repositories (written and electronic) for authoritative information such as written and electronic medical records, patient care databases, diagnostic databases, staff scheduling systems, interfaced storage archives, paper results, etc. The plan should outline the sender, inputs, usage, outputs, and receiver of information across patient care and business areas of a hospital or clinic. It should also identify the primary owner(s) for maintaining and protecting the information contained in each repository. This plan is a cross-functional effort by the IMF/C.

Chapter 4

STAFFING

4.1. General Information. One of the most difficult tasks in the AFMS today is appropriately staffing MIS Flights. The number and complexity of systems supported in the AFMS has significantly increased. MIS Flight manpower varies based on size, type, scope and needs of each MTF. To bring stability to this process the MIS Flight Commander or equivalent should proactively assess MIS programs and responsibilities and discuss manpower needs and options with his/her commander and RMO. Guidance on manpower requirements can be found in Functional Account Code 5570. Realistic and sensible manpower adjustments should be made over time to match MIS operational demands.

4.2. Staffing Considerations. The MIS Flight Commander or equivalent should establish a balance between IT support, IA responsibilities and IM services based on the organization's needs and executive team's vision. Staffing a network administrator, senior technician, and full-time government manager is a general guideline to meet minimum capabilities at smaller facilities. MIS Flights in medium and large-sized MTFs generally have more IT systems and IM demands. Medium and large inpatient facilities should consider resourcing staff to facilitate data analysis, decision support, data quality services, and 24 hour helpdesk coverage. Other factors to consider in MIS staffing are the availability of MIS Extenders (See Chapter 3), 4A0X1 Air Force Specialty Code authorizations, and government personnel for Quality Assurance Personnel contractor oversight. It is important to maintain adequate staffing ratios (MIS support staff/total MTF personnel) and IM/IT skill mix by monitoring authorized UMD positions filled by the following types of personnel options:

4.2.1. Military. MIS flights should maintain enough military positions essential to sustain MIS operations during contingency operations and extended deployment situations.

4.2.2. Civil Service. Consider staffing key MIS positions with Civil Service personnel to ensure continuity of operations and mitigate impact of military and contractor staff turnover.

4.2.3. Contractors. Contracted staff can be considered to augment operations when mission accomplishment is jeopardized by shortage of Military and Civil Service personnel/positions.

Chapter 5

IT ASSET MANAGEMENT

5.1. Overview. Asset management falls under the authority of AFI 33-112, Information Technology Hardware Asset Management, AFPD 33-1, Information Resources Management, and AFPD 23-5, Reusing and Disposing of Materiel, and can be supplemented with local guidance. There are many terms associated with hardware assets in these guides, but for simplicity this instruction will use the common term Automated Data Processing Equipment (ADPE). MIS Flight staff must be familiar with the varying types of ADPE and the level of accountability, referenced in AFI 33-112. This document can be found on the AF Portal, referenced as the USAF IT Hardware List. The MIS Flight shall be the focal point for accomplishing, coordinating, or delegating ADPE management activities.

5.1.1. MTF ADPE Equipment Custodians (ECs) are ultimately responsible for all computer equipment assigned to the organization and must ensure sub-account ECs are appointed in accordance with applicable directives. A primary and alternate custodian shall be designated in writing; however, at some bases the level of accountability may be delegated lower. Grade requirements for ADPE ECs can be found in AFI 33-112.

5.2. Annual IT Refresh.

5.2.1. The AFMS has made a considerable investment in ADPE and continues to ensure this investment is capable of supporting current and future operational requirements. IT refresh is a process whereby portions of the inventory are replaced or upgraded each year based on technology life cycles. Replacement models are decided by AFMSA/SG6 and the MHS and ordered through AFWay, a centralized purchase vehicle. Utilization of centralized purchase vehicles and processes such as AFWay and the Quarterly Enterprise Buy are mandatory. AFMOA and MTF CIOs must maintain awareness of purchase vehicle and process changes.

5.2.2. The main factors considered when setting annual refresh allotments are total MTF staffing, clinical users, exam rooms, and staff to printer ratios. During the IT annual data call requests for additional items may be submitted to MAJCOM/AFMOA with a specific mission reason for the requirement change. IT refresh allotment validation will be accomplished through AFMOA/MAJCOMs and will take place each fiscal year.

5.3. Other ADPE and Non-ADPE Procurement.

5.3.1. Non-centrally procured ADPE is budgeted, configured, and distributed by the MIS Flight. Most items are considered accountable inventory and must follow accountability procedures in accordance with governing directives listed above.

5.3.2. Many computer-related items such as paper, printer cartridges, multi-line phones, CD-RWs, uninterruptible power supply devices, overhead projectors, and telephone headsets are not restricted by the local IT procurement standards and may be obtained through local purchase processes.

5.3.3. AF/SG (AFMSA) centrally procures high-dollar systems or upgrades. For example, if the MTF has a requirement for a Picture Archiving and Communication System, the request is submitted through the appropriate organizational process for funding consideration.

5.3.4. Many medical equipment items/devices used in MTFs contain ADPE as part of a packaged system. These items are purchased through the Medical Logistics Flight using an AF Form 601, Equipment Action Request. Before these packaged systems are approved the formal request and process must include routing through the MIS Flight. This ensures equipment being purchased is validated by appropriate authorities for use on the AF Network. Coordination between the clinical staff, medical logistics, BMETs and the MIS Flight is essential.

5.3.5. Photocopiers are normally provided via a lease contract through the Defense Automated Print Service (DAPS) or procured through AFWay. Take security, energy management, and total life cycle costs into consideration when evaluating between MTF purchase and DAPS lease options for copier services. The Commander Support Staff remains the focal point for any DAPS services utilized by the MTF.

5.3.6. Cable Television, Satellite Television and Digital Satellite Systems are procured by Facility Management normally from the local CS. Organizations should be aware of MAJCOM and base restrictions.

5.3.7. LMRs are normally managed by the Medical Readiness Office (MRO). The MRO Flight Chief may enlist the help of the MIS Flight Chief or Medical Logistics Flight Commander/Facility Manager to coordinate and assist with procurement of these devices.

5.3.8. Customers requiring a Personal Electronic Device (PED) or Personal Digital Assistant (PDA) must be authorized according to local policy. The MIS Flight is the liaison to the local CS for relaying requirements, account management, and user acceptance documentation for Blackberry and similar approved network access devices.

5.4. Requirements Identification and Procurement Process. MTF staff members identify IM/IT automation requirements in general functional terms based on a need within the organization. They may provide a technical solution (brand, model number, source, and price). Requirements should be thoroughly documented (i.e. previously AF Form 3215, IT/NSS Requirements Document, now Cyberspace Infrastructure Planning System [CIPS], or latest official request format/mechanism). Requests include a proposed sustainment/support plan, (i.e. assignment of FSA, responsible owner, budget line item, etc.) and coordinated through the proper channels based on local policy.

5.4.1. MIS Flight reviews and validates requests against other MTF needs and budget limitations. If valid, the proposed solution is checked to ensure compatibility with other systems and compliance with AF network security and IA requirements. If not approved, the MIS should direct requestor to submit the requirement to the SGROCC for formal vetting, approval, and funding. Otherwise, the MIS Flight provides a technical solution or alternative recommendation identifying required resources and estimated implementation costs. Once an approved solution has been agreed upon by all parties, the MIS Flight is responsible for funding approval and implementation based on local procedures. If resources are not available, the MIS Flight submits an Unfunded Requirement to the MAJCOM/AFMOA.

5.4.2. Staff requests for purchases of networked or non-networked IT items or medical devices must be appropriately routed to, and approved by the MIS Flight. This ensures configuration control and compatibility with AF and joint systems and network security and IA requirements. IT items purchased without MIS approval should be brought to the attention of Medical Logistics, the IMF/C and the commander for corrective action.

5.4.3. DIACAP status must be considered when purchasing systems/solutions. Consult MAJCOM/AFMOA when making decisions to ensure IA timelines and planning are consistent with proposed solutions. You can find approved systems listings and other authoritative sources for Certification and Accreditation (C&A) on the Information Assurance Knowledge Exchange website at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=InformationAssurance** and the AF Enterprise-Approved Products List (E-APL).

5.5. Tracking and Inventory Management. The MIS Flight is the focal point for managing all ADPE within the MTF/DRU. The Squadron Commander or delegated representative will assign a primary and alternate ADPE custodian who may be the MTF ADPE EC or a central point of contact for all other account/subaccount ADPE ECs within the organization.

5.5.1. The MIS ADPE Manager will ensure annual inventories on all accounts are accomplished and reconciled with the local CS ECO IAW AFI 33-112. This person will also ensure that all equipment transfers and Defense Reutilization Management Office (DRMO) turn-ins are completed, documented, and validated at least annually. These turn in procedures are critical to validation of annual refresh allotments.

5.5.2. Accountable ADPE should be delivered to and initially inventoried by the local CS then signed over to the MIS ADPE Manager. After inspection, proper labeling and preparation for deployment, the ADPE is delivered and transferred to the appropriate account/subaccount ADPE EC. Both the MIS ADPE Manager and gaining EC maintain a copy of the ADPE transfer letter on file IAW their file management plan.

5.5.3. Gaining and losing ADPE ECs maintain transfer documents until inventory changes are verified and completed correctly in the local CS's automated inventory management system. The account/subaccount ADPE EC signs the new ADPE inventory listing, places a copy in the appropriate EC folder and returns the original to the MIS ADPE Manager for filing.

5.5.4. MTF hardware and software are normally purchased with Defense Health Program appropriated funds and should not be transferred to AF Line activities unless deemed to be excess and properly turned in through the Defense Reutilization Management Office (DRMO).

5.6. Report of Survey (RoS). A RoS may be required for missing, damaged or destroyed hardware. Procedures for conducting a RoS can be found in AFMAN 23-220, Reports of Survey for Air Force Property. CIOs must ensure the current ADPE ECs perform a full inventory of ADPE assets before assigning a new person to that position.

5.6.1. A RoS must be initiated IAW AFMAN 23-220 for lost, damaged or destroyed for items over $500 or if evidence of abuse, gross negligence, willful misconduct, deliberate unauthorized use, fraud, or theft is found regardless of cost. The MIS Flight contacts the MTF RoS Monitor for local procedures.

Chapter 6

INFORMATION ASSURANCE AND SECURITY

6.1. General Information. AFI 33-200, Information Assurance Management, establishes the requirement for every information system to be certified and accredited. DODI 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP) is the standard approach for identifying information security requirements, providing security solutions, and managing the security of DOD Automated Information Systems. AFI 33-210, Air Force Certification and Accreditation (C&A) Program and the Air Force Network Integration Center (AFNIC), implement DIACAP and shall be used by the Air Force to certify and accredit applications or AISs. AFMS IA guidance can be accessed through the Information Assurance KX website at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=InformationAssurance**. Air Force Network Operations Security is governed by AFI 33-115v1, Network Operations, and AFI 33-138, Enterprise Network Operations Notification. These references should be reviewed for comprehension and compliance.

6.2. Roles and Responsibilities.

6.2.1. AFMSA/SG6 serves as the single point for subject matter expertise on Certification and Accreditation (C&A) of AFMS core enterprise services, web-based software systems, applications, medical devices, and COTS products. The Chief Information Systems Security Officer (CISSO) is the AFMSA/SG6 Information Assurance Branch Division Chief and is responsible for C&A efforts within the AFMS and coordinates C&A activities for Military Health Systems/Health Affairs medical systems seeking connection the Air Force Enterprise Network.

6.2.2. CISSO Functions. The CISSO or Information Assurance Manager (IAM) Certification Function manages the certification process for AFMS systems, applications, and devices. It provides detailed step-by-step instructions to agencies and/or businesses to complete the DIACAP with specific reference to the C&A process required by the AF and DOD. Full C&A must be undertaken prior to a new system being deployed or within six months of the Authorization to Operate (ATO)/Authority to Connect (ATC) or Interim ATO/ATC (IATO/IATC) expiration. Systems must also be recertified when accredited safeguards are affected due to system changes or updates or when the operational environment or accreditation boundary has changed significantly. Some medical systems may now be certified as Platform Information Technology (PIT) packages versus individualized components requiring separate certifications. The CISSO works with AFNIC to define and identify which medical systems are classified as PIT.

6.3. C&A Process. Certification provides a formal mechanism to evaluate how well IT systems meet information security requirements, the level of risk that remains, and recommends whether or not to operate those systems at an acceptable level of risk. The C&A process incorporates the Security, Interoperability, Supportability, Sustainability, Usability (SISSU) checklist. The SISSU checklist ensures AISs are secure, supportable, sustainable, and compatible with the Air Force Enterprise Network and the Air Force IT Infrastructure. AFNIC has SISSU oversight responsibility to include certification authority (CA) signatory. AFMSA/SG6S manages the SISSU process for the AFMS. The SISSU process results in the ATO/ATC to the Air Force provisional portion of the Global Information Grid (GIG).

6.3.1. Once an ATO is granted by the Designated Approval Authority the system is entered into the Enterprise Information Technology Data Repository (EITDR) for ATC consideration. Once the ATC is issued all documents are uploaded to the AFMSA/SG6 Information Assurance KX website. These approved lists are the authoritative source for C&A and ATO/ATC status of AFMS applications and AISs.

6.4. Medical Information Security Readiness Team. AFI 41-217, Health Information Assurance for Military Treatment Facilities, requires a multi-functional medical information security readiness team. The MISRT is responsible for maintaining the integrity, availability, and confidentiality of all systems used in the MTF. The MISRT is responsible for assessing organizational IT asset threats and vulnerabilities and developing and implementing risk mitigation strategies to reduce identified threats and vulnerabilities. Automated tools (i.e. OCTAVE, RiskWatch) may be utilized for this evaluation.

6.4.1. MISRT Roles and Responsibilities.

6.4.1.1. Conducts accurate and thorough assessments of potential threats to the confidentiality, integrity, and availability of individually identifiable health information and associated information systems in the possession of the MTF, including administrative, physical, and technical vulnerabilities.

6.4.1.2. The MISRT will meet no less than quarterly and will be chaired by the HIPAA Security Officer. The MISRT chair and members will be appointed in writing, by the Medical Group Commander. Subject matter experts will be assigned to the MISRT to conduct MISRT responsibilities. At a minimum, the MISRT will include the HIPAA Security Officer (HSO), the HIPAA Privacy Officer (HPO), and representatives from Patient Administration, Medical Equipment Management Office (MEMO)/Medical Logistics/Biomedical Equipment Repair, and primary patient care. Recommended members of the MISRT include the MTF CIO, MIS Flight Chief, Facility Manager, Network Administrator, AHLTA Site Manager, FSAs, and IA manager.

6.4.1.3. Training Requirements. The MIS Flight will ensure the DOD IA Awareness computer based training is completed by each staff member annually. A completion certificate will be required to document the training.

6.4.1.4. Awareness Requirements. The MIS Flight will take advantage of the awareness notices (i.e. vulnerability, security, NOTAMs, INFOSEC etc.) provided by their local communications squadron. These notices will be forwarded to MTF personnel when available. In addition, security reminders shall be sent to MTF personnel on a monthly basis. Visual aids such as HIPAA Security Awareness posters will be positioned in staff areas throughout the MTF. The HSO will maintain an active security awareness program and ensure staff are trained IAW HIPAA guidelines.

6.4.1.5. Security Incident Management. The HSO is responsible for security incident analysis and the incidents are documented and resolved per AFI 33-138, Enterprise Network Operations Notification and Tracking.

6.4.1.6. In the event there is a suspected security incident, the MISRT will be convened to investigate and resolve the issue. If the security incident led to lost, stolen, or compromised PII or PHI, the HIPAA Security and Privacy Offices shall be notified, and the notification procedures set forth in DOD 5400.11-R, Department of Defense Privacy Program shall be followed. All steps will be taken to mitigate the effects of the incident. If there is concern about a suspected user's continued access to computer workstations or Electronic Protected Health Information (EPHI), the MIS Flight will take prompt action to suspend the individual's access to applicable systems. The HSO will provide a final report to the MTF leadership after resolution of the incident.

6.4.1.7. Contingency planning. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems containing EPHI.

6.4.2. Information Services Disaster Response Team (ISDRT). AFI 41-106, Unit Level Management of Medical Readiness Programs directs the creation of an ISDRT. In general, the team is responsible for creating network, application, and desktop computer incident response and recovery checklists and reacting to incidents or disasters causing AIS interruption or downtime. Activities should focus on protecting data, detecting and preventing further data loss or compromise, recovering and maintaining the AIS, coordinating with outside agencies to restore critical systems, and executing the recovery portion of an established Disaster Recovery Plan.

6.4.2.1. The minimum ISDRT team structure is comprised of the CIO (Team Chief), Deputy MIS Flight Commander/Chief, Flight Superintendent, Information Assurance Manager, Network Administrator, HSO, and HPO. The ISDRT may be a sub-team of the Medical Control Center (MCC). ISDRT personnel should not be assigned duties on other disaster teams and must be able to activate independently. ISDRT members may be used as manpower support when not activated.

6.4.2.2. The MISRT will identify additional critical ISDRT disaster team positions during contingencies and emergencies on an as-needed basis. Some common reasons for assembling this team: 1) major hardware failures (e.g., electrical system damage/outage, server crashes, etc.), 2) facility damage (e.g., water leak, structural damage, etc.), 3) communication systems failures (e.g., loss of network connectivity, AHLTA outages, telephone system outages, etc.), and 4) data integrity breaches (e.g., virus attacks, logical security failures, password breaches, etc.). Once activated as prescribed in the Medical Contingency Response Plan (MCRP) this team executes the MCRP Annex and corresponding checklists and reports the status of information systems at least every 12 hours to the MCC or MTF/CC.

6.4.2.3. ISDRT Roles and Responsibilities.

6.4.2.3.1. Maintain the ISDRT Annex in the MCRP and update as necessary. Gather Continuity of Operations (COOP) plans for each section, especially those critical to the continuity of patient care. COOP examples are available on the AFMOA/SGAI website at **https://vc.afms.mil/AFMOA/default.aspx**.

6.4.2.3.2. Be familiar with base Information Condition (INFOCON) level checklists and ensure the MTF complies with the current level.

6.4.2.3.3. Develop and maintain MCRP checklists. (i.e. network/desktop recovery, INFOCONs)

6.4.2.3.4. Develop annual team training schedule and conduct/document training/make-up training.

6.4.2.3.5. Ensure team recall roster is current.

6.4.2.3.6. Plan and coordinate with the Medical Readiness office on one exercise per calendar year that tests section COOP plans to ensure they are realistic, thorough, and actionable. The scenario should involve coordination of response and recovery activities after a disaster or incident that affects the MTF's ability to access/operate or control MIS. For example, an interruption in network connectivity (e.g., an increase in INFOCON levels) that disrupts access to critical information systems such as AHLTA. Coordination should include ISDRT activation and contacting partners and outside agencies to assist as needed. The annual exercise can be done in conjunction with other readiness exercises. Document exercise scenarios with after action report(s).

6.4.2.3.7. Assess damage, loss, or compromise to MIS hardware, software, and data.

6.4.2.3.8. Deny access or shut down vulnerable systems.

6.4.2.3.9. Maintain and prioritize a list of critical systems and associated administrators of those systems.

6.5. Physical and Logical Security. The MIS Flight in conjunction with MTF Facility Management is responsible for securing server rooms, communications closets, stored IT assets and creating appropriate access control lists to secure areas IAW AFI 33-101, Commanders Guidance and Responsibility. Physical security of critical IT assets prevents intrusion and sabotage of these strategic assets. Likewise the MIS flight should implement logical security measures such as file folder permissions, role based access, and account permission audits to prevent unauthorized access to information and protect data integrity.

6.6. User Network Access Compliance. Strict compliance and disciplined enforcement of user network access, information protection, and information assurance directives increases overall reliability and availability of Air Force systems. AFSSI 8522, Access to Information Systems, and its AFI references provide comprehensive guidance for licensing network users and certifying network professionals. Before individuals are given access to the af.mil or af.smil domain, specialized systems, and/or mission systems, they must have 1) a favorable background investigation and 2) completed information protection training. Users' access or privileges to network and/or applications may be revoked, suspended, and then reinstated for various reasons as described in the referenced materials.

6.7. Software and Firmware Patching and Maintenance: To protect the AF Global Information Grid, systems must "comply-to-connect" by staying updated with the latest patches and cyber security directives. TCNOs, MTOs, and Information Assurance Vulnerability Assessments (IAVAs) requiring CST, FSA, or Network Administrator patching actions are released regularly by AIS vendors, AFCERT, JTF-GNO, and the Air Force Network Operations Center. AFI 33-138, Enterprise Network Operations Notification and Tracking, covers actions and responsibilities of functional system owners with regards to MTOs, TCNOs, and IAVAs. When directed, software and firmware patches, updates, upgrades, and service packs must be applied in a timely fashion, or a Plan of Action and Milestones (POA&M) to mitigate required directive must be developed, submitted, and tracked to completion.

Chapter 7

HIPAA SECURITY

7.1. Overview. The purpose of the Health Insurance Portability and Accountability Act (HIPAA) Security program is to enhance the protection, confidentiality, integrity, and availability of personally identifiable information and protected health information as well as promote compliance with Federal, Department of Defense and Air Force mandates. This policy applies to all information systems, organizational units and military, civilian, contractor and volunteer staff working at Air Force military treatment facilities. AFI 41-217, DODR 6025.18-R, DOD Health Information Privacy Regulation, and DOD 8580.02-R, DOD Health Information Security Regulation, will assist Medical Information Systems personnel in administering this program. Additionally, DOD and Air Force implementation of the provisions of The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, remain undetermined and may eventually affect MIS operations.

7.2. Medical Group HIPAA Security Officer (HSO) Roles and Responsibilities.

7.2.1. The HSO, either CIO or contractor, will work with local representatives from the communications squadron as well as medical information systems team members to assist with information protection and operational requirements.

7.2.2. The HSO may invite other members of the MTF to participate in workgroups, taskforces, or committees in support of protecting individually identifiable health information and associated information systems.

7.2.3. Functions as the liaison between the MTF, higher headquarters, base Information Assurance Office, and other internal and external organizations in developing, implementing, and maintaining the military treatment facility health information security program.

7.2.4. Convenes and coordinates the Medical Information Security Readiness Team. (See Chapter 6, Information Assurance and Security, Paragraph 6.4)

7.2.5. Implements administrative, physical and/or technical safeguards sufficient to reduce risks and vulnerabilities to PHI and associated information systems to a reasonable and appropriate level as specified by relevant Federal, DOD and Air Force instructions, publications, and regulations.

7.2.6. Works with the HIPAA Privacy Officer to monitor medical group contracts to ensure those contracts that involve the exposure to or handling of PHI or electronic PHI by third parties includes TRICARE Management Activity's approved Business Associate Agreement and appropriate HIPAA Security language.

7.2.7. Ensures applicable publications and procedures are periodically reviewed and revised when changes occur.

7.2.8. Continuously assesses, implements, monitors, and revises the medical group health information assurance posture as part of overall management of the host base network infrastructure.

Chapter 8

INSPECTIONS

8.1. General Information. The IMF/C is a logical point to track and coordinate organizational compliance with IM regulatory requirements. MIS leadership needs to be familiar with these requirements, educate the staff, and help ensure requirements are met.

8.2. Self-Inspection Program. Self-inspections are primarily compliance based and conducted using checklists comprised of requirements from governing directives such as this AFI. The Air Force Inspection Agency (AFIA) maintains various checklists relating to inspectable areas defined by the Health Services Inspection program. These checklists can be utilized to help build the MIS self-inspection checklist, and can be found on the AFIA website on the Air Force Knowledge Now website at **https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=AFIAMedOps**. The checklist are updated with the release of new inspection standards from governing agencies to include HSI, Joint Commission, and Accreditation Association of Ambulatory Health Care, as well as when governing publications are updated or replaced.

8.2.1. A self inspection is performed within 60 days of entering a management position. Open items must be updated to Quality Assurance personnel every six months to show resolution efforts and verify that documentation exists to support improvement and compliance. A follow on inspection should be done annually and/or with major revisions to the self-inspection checklist.

8.2.2. All levels of management are accountable for identifying and correcting mission performance problems. When a deficiency is found, it must be documented and properly tracked. A corrective action plan, including the identification of the deficiency, planned or taken corrective actions, estimated completion date, and OPR is required.

8.2.3. Reports from previous inspections should be reviewed. These reports list overall outcome as well as findings, deficiencies, or recommended improvement areas. Inspectors may review these previous reports prior to their visits and specifically look for repeat findings in the same areas.

8.3. Special Interest Items. Inspections teams/agencies may advertise increased emphasis on certain aspects of a program or process. These are referred to as special interest items. The IMF/C and MIS Flight leadership should note special interest items applicable to IM/IT/IS and focus attention on any special reporting or documentation steps for these items to ensure compliance.

8.4. Inspection Types. There are several inspections that evaluate MTF MIS functions.

8.4.1. Civilian. The JC and AAAHC assess all of the major functions of medical treatment facilities. Ambulatory clinics fall under AAAHC whereas bedded facilities fall under JC. JC may contact the organization with no prior notice to the inspection start date. These agencies examine performance of processes and support functions that most significantly impact the quality of patient care. The standards do not always specify how the function or process is to be completed, but focus on the effects and outcomes of those processes on patient care.

8.4.2. Health Services Inspection. AFIA HSI inspection usually complements a JC or AAAHC accreditation inspection. Inspection criteria for this area are similar to those of civilian organizations, but are based more on compliance with Air Force Instructions (AFIs) and other guidance.

8.4.3. Operational Readiness Inspection (ORI). Similar to the HSI, the ORI is primarily compliance based and, reviews the organization's ability to meet operational readiness and emergency planning requirements. This assessment ensures organizations are performing their specified mission and verifies they are prepared for contingency and/or emergency situations. MIS Flights may be called upon to demonstrate information protection activities and responses such as actions taken during an elevated INFOCON.

8.4.4. Command Cyber Readiness Inspections (CCRIs). CCRIs, previously called Defense Information Systems Agency (DISA) Enterprise Compliance Visits, are assessments of information assurance readiness and cyber security posture around key DOD policies and configuration requirements. Three possible grades are: No Concerns (Never accomplished), Compliance/Monitor (common), and GIG Vulnerability Alert (circuits shut down/base isolated...rare but possible). These installation compliance visits are conducted by teams from DISA who scan networks and measure compliance with DISA Security Technical Implementation Guides (STIGs), and network, server, and computer security requirements. Similar to the ORI, some CCRI findings require follow-up corrective action.

8.5. Inspection Time. MIS Flights that document well, continually review self-inspection checklists, and check special interest items are normally prepared for an inspection. Inspectors look for examples of best practices within the organization. Best practices are examples where a unit has gone above and beyond the standard level of performance, customer service, or available services. Inspections are excellent opportunities for MIS Flights to highlight such areas.

Chapter 9

DEPLOYABLE UNIT MANAGEMENT REQUIREMENTS

9.1. Overview. MIS personnel will deploy to a variety of forward operating locations in support of contingency, exercise, and deployment operations. Operations range from an established base to stand-alone medical capability where no other military presence is co-located. MIS professionals must be trained/certified and able to respond to these situations.

9.1.1. General Roles. Medical Service Corps officers (MSCs) and Health Services Managers (4A0X1s) play a major role while deployed with a special focus on assisting the medical commander with MIS support. They provide information systems connectivity and other crucial aspects of MIS management in the absence of adequate host-base and/or remote communications/AIS support. At most locations, units within the Expeditionary Combat Support (ECS) provide core IT services while MIS staff performs CST duties and medical FSA AIS support.

9.1.2. MIS Responsibilities. Deployed MIS staff collects, maintains and retrieves timely and accurate information for planning, organizing, and directing support operations. The nature of these duties makes it critical that control mechanisms are implemented to protect sensitive information and data. Responsibilities vary greatly based on the tasking and deployed location, however, deployed members are commonly required to perform duties normally required of an in-garrison CST as well as providing hands-on FSA support to a variety of deployed-health AIS's.

9.2. Proper Control Processes. Written guidelines and policies must be followed to safeguard computer systems and information against damage or compromise. Work closely with the ECS and other support personnel to limit mission degradation due to MIS downtime or misuse.

9.3. Types of Deployment Locations.

9.3.1. Existing Deployment Location. Under most circumstances, the MTF deploys a personnel package to assume responsibility of an existing medical unit. An inventory and status of existing equipment shall be performed by the new OIC/NCOIC as soon as possible and any missing, damaged, or obsolete equipment shall be identified to the Area Of Responsibility AF Forward Surgeon Staff or appropriate Joint Task Force authority for accountability and replacement. Currency of software applications will be managed through network tasking orders issued by the theater's controlling network operations center.

9.3.2. New Deployment Location. When deploying to a bare-base location, the personnel Unit Type Code (UTC) requires a deployable ADPE package and MIS personnel. The ADPE package may include server(s), laptops, printers, bar-code readers/scanners, and various network and communication devices. The deployed MIS personnel are responsible for initial setup and configuration of the MIS equipment. Reach-back voice communication will be established with the Iridium satellite phone and networked data services by connecting to the ECS grid.

9.3.3. Redeployment. Depending on the mission, the deployed Expeditionary Medical Group (EMDG) communication and information processing equipment may remain in place or be redeployed to the UTC generation (home station) unit. In either case, a deployment termination inventory of all ADPE must be completed prior to return to the generating unit or assumption of the new EMDG Commander. MIS staff must ensure systems are properly archived and wiped or reformatted to protect health information.

9.3.4. Humanitarian Support. Similar to a new deployment location, humanitarian missions require a large commitment of organic MIS skills and equipment. Medical personnel may be the only military resources in the area and all communication and information services may come from and be supported by Air Force medical personnel and equipment.

9.4. Deployed Resources. The variability of deployment locations, taskings, and Joint Service issues make planning for deployed resources challenging. The best planning strategy is to (1) know the MTF's Designed Operational Capability tasked UTCs, Air Expeditionary Force (AEF) cycle, and existing EMDG presence, (2) establish communication with the current deployed MSC and 4A0X1 or designated EMDG MIS Flight Commander or NCOIC and (3) inquire as to what resources are available (4) talk with the Manpower and Equipment Force Packing agent for the UTC. The MTF's supporting MAJCOM readiness division is a recommended initial source for this information.

9.5. Maintenance. For MTFs tasked with a deployable equipment package, the MIS Flight Commander, in conjunction with the MRO and the Medical Logistics Flight Commander, creates and executes a maintenance and upkeep plan for all deployable ADPE. This activity includes loading all software packages offered to date by the AFNIC, AFMSA, and deployable application program offices, as appropriate. Maintenance on deployable ADPE is performed at least annually, during Phase II exercises, or upon a deployment warning order.

9.6. Training. Training requirements vary based on UTC mission and AEF rotation. Due to the unpredictability of deployment location and base communication squadron support, deploying MIS personnel should be trained on a wide variety of communication and information processing equipment. Additional training on deployment unique applications, such as; Theater Medical Information Program, TRANSCOM Medical Regulating and Command and Control Evacuation System, Joint Patient Tracking Application, Joint Medical Work Station, and Tactical Satellite communication systems may be required. A familiarity with network communication devices (switches, routers, etc) is advisable. UTC specific training requirements can be found in the UTCs Air Force Tactics, Techniques, and Procedures.

9.6.1. Training Resources. Just-in-time training for deploying units is available and is facilitated by the MRO and appropriate MAJCOM tasking organization. The Expeditionary Medical Support basic course is the primary focus for just-in-time training; however, other training resources may be available through the MTF, MAJCOM/AFMOA and Gunter. Training resources may also be available through the local CS. It is recommended that training requirements be listed in the SLA between the MTF and the CS. Operational Readiness Phase I and II exercises are excellent opportunities to train on deployable communication and information processing equipment and applications. Specialized training may be required for new programs and is normally identified within personnel tasking order.

Chapter 10

PARTNERSHIPS AND SERVICE LEVEL AGREEMENTS

10.1. Partnerships. Providing robust MIS support requires a collaborative and coordinated effort between various agencies. The MIS staff is responsible for establishing partnerships with key IM/IT service providers. The Communications Squadron (CS) and its service line Flights (NCC, CFP, Asset Management, LMR, Telephone Ops) are the primary local service providers and must be strategic partners in MIS activities. CIOs and MIS Flight staff members must meet with CS counterparts regularly and work to develop a mutual understanding of mission requirements.

10.2. Service Level Agreement. SLAs provide a tool to enhance effective, efficient, and reliable end-to-end customer support programs and clearly outline desired results for all parties involved. AFI 33-115, Volume 1, Network Operations, specifies that SLAs should be used when additional services or unique response times exceed services specified as standard service levels. Standard service levels, as they relate to core services, specify basic services and response times offered to all base local area network customers. NCCs should operate 24-hours-a-day, 7-days-a-week in person or on call. As services are centralized away from NCC/CFP control, higher level SLAs may supersede local SLAs.

10.2.1. MTFs with inpatient care or 24/7 operations must ensure any SLA addresses after-hours and weekend support from the NCC. Due to the net-centric nature of diagnostic equipment, harm to patients could occur if a problem is not addressed quickly. The SLA may include, but is not limited to, network service availability rates, fault response times, configuration change procedures, initial contingency support requirements, customer escalation, security management procedures, and shared helpdesk, maintenance, and administration responsibilities. The SLA should be signed by the MTF/CC and the CS/CC. (See Attachment 2 for a Sample Local SLA Outline)

10.2.2. The SLA should not include payment for services provided to other organizations by local CS. This is a violation of defense health funding appropriation law and regulations; medical funds (2X) can only be used for medical operations. If a local CS has requested fee-for-service reimbursement, discuss the situation with your RMO, MAJCOM/AFMOA and Base Legal Office.

10.3. HIPAA Agreements. HIPAA requires that personnel with access to PHI take certain precautions prior to disclosure. All personnel with access to PHI require a certain degree of training that varies with their relationship to the information. Even though the NCC and base CS have certain capabilities, such as the ability to remotely view what is on an individual’s monitor and the contents of network traffic, they are viewed as information custodians and not required to accomplish HIPAA training annually.

CHARLES B. GREEN, Lt General, USAF,
MC, CFS
Surgeon General

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 16-14, Information Protection, 28 September 2010

AFPD 23-5, Reusing and Disposing of Materiel, 26 March 2001

AFMAN 23-220, Reports of Survey for Air Force Property, 1 July 1996

AFI 31-501, Personnel Security Program Management, 27 January 2005

AFPD 33-1, Information Resources Management, 27 June 2006

AFI 33-101, Commanders Guidance and Responsibilities, 18 November 2008

AFI 33-112, Information Technology Hardware Asset Management, 20 April 2006

AFI 33-114, Software Management, 13 May 2004

AFI 33-115, Volume 1, Network Operations (NETOPS), 24 May 2006

AFI 33-115, Volume 2, Licensing Network Users and Certifying Network Professionals, 14 April 2004

AFI 33-119, Air Force Messaging, 24 January 2005

AFI 33-129, Web Management and Internet Use, 3 February 2005

AFI 33-138, Enterprise Network Operations Notification and Tracking, 28 November 2005

AFI 33-200, Information Assurance (IA) Management, 23 December 2008

AFI 33-210, Air Force Certification and Accreditation (C&A) Program, 23 December 2008

AFPD 33-3, Information Management, 28 March 2006

AFI 33-332, Privacy Act Program, 29 January 2004

AFMAN 33-363, Management of Records, 1 March 2008

AFI 36-2101, Classifying Military Personnel (Officer and Enlisted), 14 June 2010

AFI 36-2201, Volume 3, Air Force Training Program, 15 September 2010

AFI 41-106, Unit Level Management of Medical Readiness Programs, 14 April 2008

AFI 41-210, Patient Administration Functions, 22 March 2006

AFI 41-217, Health Information Assurance for Military Treatment Facilities, 23 December 2005

AFI 64-117, Air Force Government-Wide Purchase Card (GPC) Program, 31 January 2006

AFSSI 8522, Access to Information Systems, 9 June 2008

CJCSM 6510.01E, Information Assurance (IA) and Computer Network Defense, 15 August 2007

DOD 6025-18R, DOD Health Information Privacy Regulation, 24 January 2003

DODI 8260.04, Military Health System (MHS) Support to DOD Strategic Analysis, 18 December 2009

DODD 8500.01E, Information Assurance (IA), 24 October 2002

DODI 8510.01, DOD Information Assurance Certification and Accreditation Process, 28 November 2007

DOD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005

DOD 8580.02-R, DOD Health Information Security Regulation, 12 July 2007

Public Law 104-13, Paperwork Reduction Act of 1995, 22 May 1995

Abbreviations and Acronyms

AAAHC— Accreditation Association for Ambulatory Health Care

ADPE— Automated Data Processing Equipment

AEF— Air Expeditionary Force

AF— Air Force

AFGIG— AF Global Information Grid

AFI— Air Force Instruction

AFIA— Air Force Inspection Agency

AFMAN— Air Force Manual

AFMOA— Air Force Medical Operations Agency

AFMS— Air Force Medical Service

AFMSA— Air Force Medical Support Agency

AFNIC— Air Force Network Integration Center

AFSPC— Air Force Space Command

AHLTA— Armed Forces Health Longitudinal Technology Application

AIS— Automated Information System

ATC— Authority to Connect

ATO— Authorization to Operate

BMETs— Biomedical Equipment Repair Technicians

CCRI— Command Cyber Readiness Inspection

CFP— Communications Focal Point

C&A—Certification and Accreditation

C&I— Communications and Information

CIO— Chief Information Officer

COOP— Continuity of Operations Plan

COTS— Commercially off-the-shelf

CS— Communications Squadrons

CST— Client Support Technicians

CSO— Chief Security Officer

DAPS— Defense Automated Print Service

DIACAP— DOD Information Assurance Certification and Accreditation Process

DISA— Defense Information Systems Agency

DOD— Department of Defense

DRMO— Defense Reutilization Management Office

DRU— Direct Reporting Units

APL— Enterprise-Approved Products List

EAS— Expense Assignment System

EC— Equipment Custodian

ECS— Expeditionary Combat Support

EMDG— Expeditionary Medical Group

EPHI— Electronic Protected Health Information

FOA— Field Operating Agency

FSA— Functional System Administrator

GIG— Global Information Grid

GOTS— Government off-the-shelf

HIPAA— Health Insurance Portability and Accountability Act

HIT— Healthcare Information Technology

HSI— Health Services Inspection

HSO— HIPAA Security Officer

IA— Information Assurance

IATO/IATC— Interim ATO/ATC

IAVA— Information Assurance Vulnerability Assessments

IM— Information Management

IMF/C— Information Management Function/Committee

IMP— Information Management Plan

INFOCON— Information Condition

INOSC— Integrated Network Operations and Security Center

IS— Information Services

ISDRT— Information Services Disaster Response Team

IT— Information Technology

JC— Joint Commission

KX— Knowledge Exchange

LAN— Local Area Network

LMRs— Land Mobile Radios

LSMTF— Limited Scope Medical Treatment Facility

MAJCOM— Major Command

MCC— Medical Control Center

MCiS— Medical Cyber Infrastructure Services

MCRP— Medical Contingency Response Plan

MDG— Medical Group

MEMO— Medical Equipment Management Office

MHS— Military Health System

MIS— Medical Information Services

MISRT— Medical Information Security Readiness Team

MRO— Medical Readiness Office

MSC— Medical Service Corps Officer

MSIM— Medical Systems Infrastructure Modernization

MTF— Medical Treatment Facility

MTO— Maintenance Tracking Order

NCC— Network Control Center

NCOIC— Non Commissioned Officer in Charge

NOTAMs— Notices to Airmen

OIC— Officer in Charge

OODA— Observe, Orient, Decide, Act

OPR— Office of Primary Responsibility

ORI— Operational Readiness Inspection

PDA— Personal Digital Assistant

PED— Personal Electronic Device

PHI— Protected Health Information

PII— Personally Identifiable Health Information

PIT— Platform Information Technology

PM— Program Managers

PMO— Program Management Office

RAT— Requirements Assessment Team

RoS— Report of Survey

RMO— Resource Management Office

SAV— Staff Assistant Visit

SG— Surgeon General

SGROCC— Surgeon General's Requirements for Operational Capabilities Council

SISSU— Security, Interoperability, Supportability, Sustainability, Usability

SLA— Service Level Agreement

SLCM— System Lifecycle Management

SME— Subject Matter Expert

SSG— Standard Systems Group

STIG— Security Technical Implementation Guides

TCNO— Time Compliance Network Order

TELMOD— Telephony Modernization

TMA— TRICARE Management Activity

UMD— Unit Manning Document

UTC— Unit Type Code

WWW— Website URL Index

AFMOA—https://vc.afms.mil/AFMOA/default.aspx

AFMOA—https://vc.afms.mil/AFMOA/default.aspx

Air Force Publishing/e-Publishing website: http://www.e-publishing.af.mil

Air Force Records Disposition Schedule:
https://www.my.af.mil/afrims/afrims/afrims/rds/rds_series.cfm

SGROCC: https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=SGROCC

AFMS CIO Knowledge Junction:
https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=AFMSChiefInfoOfficer

AFMS CIO Community of Interest: https://kx.afms.mil/community/community/afmscio

Data Quality: http://www.tricare.mil/ocfo/mcfs/dqmcp/management_control.cfm

Air Force Surgeon General's Commander Action Group–AFMS Medical Futures Support Plan: https://kx.afms.mil/sgcag

Air Force Inspection Agency—
https://kx.afms.mil/kxweb/dotmil/kj.do?functionalArea=AFIAMedOps

Air Force Information Technology E-Learning/Skillport:
https://www.my.af.mil/skillportcbtprod4/skillportfe/main.action?selectedTab=1

Attachment 2

SAMPLE LOCAL SERVICE LEVEL AGREEMENT OUTLINE

(Example Outline Only: Not Mandatory Format)

DD MMM YY

MEMORANDUM FOR RECORD FOR XXX CS/CC AND XXX MDG/SGSI

FROM: XXX MDG/CC
111 Any Street
XYZ AFB SS 99999-999

SUBJECT: SAMPLE Service Level Agreement (SLA) between XXX CS & XXX MDG/SGSI

1. PURPOSE

2. SCOPE

3. PARTIES TO SERVICE LEVEL AGREEMENT

4. PHYSICAL NETWORK

   A. DEMARCATION.

   B. INSTALLATION AND INITIAL CONFIGURATION.

   C. HARDWARE OWNERSHIP.

   D. HARDWARE CHANGES, UPGRADES, OR RELOCATION.

   E. PHYSICAL ACCESS AND SECURITY.

   F. AUTOMATED DATA PROCESSING EQUIPMENT (ADPE) MANAGEMENT.

   G. JOINT PARTNERSHIP ARRANGEMENTS (Army, Navy, BRAC, Universities, VA)

5. MAINTENANCE, HELPDESK AND TROUBLESHOOTING SUPPORT

   A. GENERAL IT SUPPORT STRUCTURE.

   B. MAINTENANCE.

   C. HELPDESK TICKETS.

   D. TICKET RESPONSE TIMES AND PRIORITIES.

   E. TICKET RESOLUTION ELEVATION PROCEDURES.

6. NETWORK ADMINISTRATION

   A. ACTIVE DIRECTORY & GROUP POLICIES.

   B. USER, CST, FSA & MEDICAL NET ADMIN RIGHTS AND PRIVILEGES

   C. PATCHES, UPGRADES, GPO CHANGE COORDINATION PROCESS.

   D. WIRELESS CONTROLLER ADMINISTRATION.

   E. LAN CORE AND REMOTE SWITCH CONTROL AND ADMINISTRATION.

F. NETWORK PERFORMANCE AND CONNECTIVITY.

G. BASE MAINTENACE OUTAGE COORDINATION.

7. INFRASTRUCTURE FOR FAILOVER MITIGATION

8. ADDITIONAL NETWORK AND CLIENT SUPPORT RESPONSBILITIES

9. CAPITAL PLANNING, EXECUTION AND REIMBURSEMENTS

10. RESOLUTION AND REVIEW TIMELINE STATEMENT

11. SIGNATURE BLOCKS